UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. DEREK WAYNE RONDEAU, Defendant.	4:23-CR-40004-KES ORDER ADOPTING IN PART AND DENYING IN PART REPORT AND RECOMMENDATION AND GRANTING RONDEAU'S MOTION TO SUPPRESS

The Government filed an indictment against defendant, Derek Wayne Rondeau, which charges Rondeau with two counts of production of child pornography in violation of 18 U.S.C. §§ 2251(a) and 2251(e), and two counts of kidnapping in violation of 18 U.S.C. § 1201(a)(1). *See* Docket 1. Rondeau moves to suppress all evidence obtained from a search of his Apple ID(s) and iCloud account(s). *See* Docket 30. Rondeau also moves to suppress the statements he made to officers after he was arrested but prior to being advised of his *Miranda* rights. *Id.*

The court referred Rondeau's motion to a Magistrate Judge under 28 U.S.C. § 636(b)(1)(B). After holding an evidentiary hearing, the Magistrate Judge recommended Rondeau's motion to suppress be denied in part and granted in part. *See* Docket 44. Specifically, the Report and Recommendation recommended denying Rondeau's motion to suppress evidence obtained from Rondeau's iCloud account. *See id.* at 24. The Report and Recommendation recommended granting Rondeau's motion to suppress the statements Rondeau

made "in response to questions about the location of his phone, truck, or other aspects of the alleged crime while in custody and prior to the advisement of his *Miranda* rights." *Id.* at 15. Rondeau timely filed objections to the Report and Recommendation. Docket 48. After a de novo review of the Report and Recommendation and the record, the court issues the following order.

LEGAL STANDARD

This court's review of a magistrate judge's report and recommendation is governed by 28 U.S.C. § 636 and Rule 72 of the Federal Rules of Criminal Procedure. The court reviews de novo any objections to the magistrate judge's recommendations with respect to dispositive matters that are timely made and specific. 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 72(c). Because motions to suppress evidence are considered dispositive matters, a magistrate judge's recommendation regarding such a motion is subject to de novo review. 28 U.S.C. § 636(b)(1); *see also United States v. Raddatz*, 447 U.S. 667, 673 (1980). In conducting a de novo review, this court may then "accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge." 28 U.S.C. § 636(b)(1); *see also United States v. Craft*, 30 F.3d 1044, 1045 (8th Cir. 1994).

FACTS

After a de novo review of the transcript of the evidentiary hearing and the exhibits received into evidence, the court adopts the facts as set forth in the Report and Recommendation. Rondeau did not file any objections to the facts.

DISCUSSION

Rondeau makes two objections to the Report and Recommendation. *See* Docket 48. First, Rondeau objects to the Report and Recommendation's conclusion that the warrant for the iCloud account was sufficiently particular. *Id.* at 2. Rondeau argues that the warrant was overly broad, provided no limitations or guidance to executing officers, and allowed officers to rummage through Rondeau's iCloud account. *Id.* at 3. Second, Rondeau objects to the Report and Recommendation's application of the *Leon* good faith exception to the exclusionary rule. *Id.* Rondeau agrees that the warrant lacked probable cause but argues that the *Leon* good faith exception should not apply because law enforcement did not act in an objectively reasonable manner in relying on the warrant. *Id.* at 4-6. The court addresses Rondeau's objections in turn.

I. Rondeau's First Objection: The Magistrate Judge Erred in Concluding that the Warrant for the iCloud Account was Sufficiently Particular.

Before addressing Rondeau's argument that the iCloud warrant was not sufficiently particular, the court first addresses the Report and Recommendation's finding that the iCloud warrant was not supported by probable cause. *See* Docket 44 at 21 (finding the warrant lacked probable cause and was thus invalid).

A. Probable Cause

The Report and Recommendation concluded that the iCloud warrant was issued without probable cause because the affidavit did not establish "a nexus between Mr. Rondeau's alleged criminal conduct and the broad array of data

sought by the warrant." Docket 44 at 20-21. Rondeau agrees with the Magistrate Judge's conclusion and the Government has not filed an objection. *See* Docket 48 at 1. The court holds that while probable cause existed for officers to search Rondeau's iCloud account, the list of items officers sought to seize exceeded the probable cause that existed for the iCloud warrant.

"To be valid under the Fourth Amendment, a search warrant must be supported by a showing of probable cause." *United States v. Wallace*, 550 F.3d 729, 732 (8th Cir. 2008) (quoting *United States v. Summage*, 481 F.3d 1075, 1077 (8th Cir. 2007)). A warrant is supported by probable cause if the totality of the circumstances demonstrates "a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Ivey*, 91 F.4th 915, 917 (8th Cir. 2024) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). Further, there must "be a nexus . . . between the item to be seized and [the] criminal behavior." *United States v. Saddler*, 19 F.4th 1035, 1039 (8th Cir. 2021) (alternation in original) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)).

The sufficiency of a search warrant affidavit is examined using "common sense and not a hypertechnical approach." *United States v. Grant*, 490 F.3d 627, 632 (8th Cir. 2007) (cleaned up and citations omitted). Thus, "[w]hen the [issuing judge] relied solely upon the supporting affidavit to issue the search warrant, only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause." *United States v. O'Dell*, 766 F.3d 870, 874 (8th Cir. 2014) (second alteration in

original) (quoting *United States v. Solomon*, 432 F.3d 824, 827 (8th Cir. 2005)). Here, the record indicates that the state magistrate judge who issued the warrant relied solely on Detective Nelson's affidavit in support of the search warrant. *See* Docket 39 at 22. Thus, the court's probable cause analysis is limited to the information contained in Detective Nelson's affidavit.

The court agrees with the Magistrate Judge's finding that Detective Nelson's affidavit in support of the search warrant of Rondeau's iCloud account provided sufficient facts from which the issuing judge could find probable cause to believe Rondeau's iCloud account contained evidence relating to the rape of S.R. *See* Docket 44 at 19-20; *see also United States v. Daigle*, 947 F.3d 1076, 1082 (8th Cir. 2020) (holding that a victim's statement that evidence of a sexual assault exists on a device is sufficient to support probable cause to search that device for that evidence). Based upon S.R.'s statements that Rondeau took photos and videos of her during the alleged rape and the officers' connection of Rondeau's iPhone to the iCloud account, Docket 39 at 16, the issuing state magistrate judge had a substantial basis for concluding that there was a fair probability that evidence of the alleged rape would be on Rondeau's iCloud account. Thus, the requisite nexus existed between the crime and the iCloud account to support a finding that the iCloud warrant was supported by probable cause.

The Magistrate Judge concluded, however, that the affidavit for the iCloud warrant failed to establish a nexus between "Rondeau's alleged criminal conduct and the broad array of data sought by the warrant," because it lacked

sufficient temporal limitations and sought to seize items unrelated to the crime under investigation.[1] Docket 44 at 20-21. As noted in the Report and Recommendation, the affidavit for the iCloud warrant requested the seizure of certain groups of data based on what the data "can" or "may" do. *See id.* at 20 (listing some provisions of the warrant's affidavit describing evidence that "may lead to the discovery of additional evidence" or "may also provide relevant insight into the account owner's state of mind"). The court agrees with the Magistrate Judge that not every item listed as an item to be seized was supported by probable cause because not every item was supported by a reasonable belief "that the evidence sought will aid in a particular apprehension or conviction." *See Saddler*, 19 F.4th at 1039 (quoting *Warden*, 387 U.S. at 307).

As the Magistrate Judge reasoned, "[n]othing in the facts supplied by Detective Nelson gives any indication that a spreadsheet, an email, a game, Mr.

[1] Because temporal limitations typically play a role in the particularity analysis, the court addresses that issue below. *See United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (discussing that a social media warrant would have been more particular if it had "requested data only from the period of time during which [the defendant] was suspected of taking part in the [charged crime]"); *United States v. Hernandez*, 2010 WL 26544, at *11 (S.D.N.Y. Jan. 6, 2010) (noting that a "temporal limitation" is an "indici[um] of particularity") (alteration in original and citation omitted). As the Magistrate Judge noted in the Report and Recommendation, however, despite Officer Stroschein's testimony that she cannot "take things at face value" regarding when S.R. reported her first communication with Rondeau, *see* Docket 44 at 4, S.R.'s allegations did not provide probable cause to search and seize data created as early as 2011—when the iCloud account was created—because there is no nexus "between the item to be seized and [the] criminal behavior." *Saddler*, 19 F.4th at 1039 (citation omitted).

Rondeau's calendar from 2018, or the majority of the 'millions of digital artifacts' in the iCloud file relate in any way to the investigation of the rape of S.R. in mid-June, 2022." Docket 44 at 21. As such, this court concludes that the search and seizure of Rondeau's 11-year-old iCloud account was "broader than can be justified by the probable cause upon which the warrant was based." *United States v. Burkhow*, 2020 WL 589536, at *8 (N.D. Iowa Feb. 6, 2020) (quoting *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013)).

B. Particularity

The Report and Recommendation found that the search warrant was sufficiently particular in describing the items to be seized because the warrant, while "exhaustive," provided a list of eleven types of data to be seized, which left little doubt as to the data sought. *See* Docket 44 at 17. Rondeau argues that the list of items to be seized fails the particularity requirement because it "provided no limitations or guidance to officers regarding what data they could search once the iCloud data was received from Apple . . . [r]ather, it authorized law enforcement to conduct a general rummaging through the entirety of Rondeau's iCloud." Docket 48 at 2-3. As discussed below, the court agrees. The warrant lacks sufficient particularity because it does not limit the files for which the iCloud account is to be searched and which are to be seized.

The Fourth Amendment mandates that "no Warrants shall issue . . . [unless] particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend IV. The Fourth Amendment requires that "those searches deemed necessary should be as limited as possible."

Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "The particularity requirement prohibits officers 'from conducting general, exploratory rummaging of a person's belongings.' " *United States v. Shrum*, 59 F.4th 968, 973 (8th Cir. 2023) (quoting *United States v. Sigillito*, 759 F.3d 913, 923 (8th Cir. 2014)).

Courts evaluate compliance with the particularity requirement according to "a standard of 'practical accuracy' rather than a hypertechnical one." *Summage*, 481 F.3d at 1079 (quoting *United States v. Peters*, 92 F.3d 768, 769-70 (8th Cir. 1996)). "To satisfy the particularity requirement of the [F]ourth [A]mendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized." *United States v. Sherman*, 372 F. App'x 668, 675 (8th Cir. 2010) (quoting *Summage*, 481 F.3d at 1079). The items to be seized "must be described with sufficient particularity as to enable the searcher to locate and identify the . . . items with reasonable effort and to avoid mistakenly . . . seizing the wrong items." *United States v. Gleich*, 397 F.3d 608, 611 (8th Cir. 2005). The requisite specificity of a warrant depends upon "such factors as the purpose for which the warrant was issued, the nature of the items to which it is directed, and the total circumstances surrounding the case." *United States v. Fiorito*, 640 F.3d 338, 346 (8th Cir. 2011) (quoting *Milliman v. Minnesota*, 774 F.2d 247, 250 (8th Cir. 1985)).

Here, the court agrees with the Magistrate Judge that the iCloud warrant particularly described the place of the search. *See United States v. Skarda*, 845 F.3d 370, 377 (8th Cir. 2016) (requiring that the description be "sufficient[ly]

particular as to enable the executing officer to locate and identify the premises with reasonable effort" and limit the "reasonable probability that another premise might be mistakenly searched"). Regarding the description of the items to be seized, however, the court agrees with Rondeau's assertion that the iCloud warrant was not sufficiently particular in its description of the items to be seized because the warrant was not as particular as the circumstances of the case allowed.

For iCloud warrants in general, while it is not clear how "an iCloud warrant should identify the target of a search with particularity," a warrant may do so through subject matter limitations—for example, limiting the "search of communications data to only communications with known or suspected co-conspirators," or through temporal limitations. *United States v. McCall*, 84 F.4th 1317, 1327 (11th Cir. 2023). "Because the same content can be stored in so many different formats, a subject-based limitation may sometimes be so broad as to be meaningless." *Id.* Thus, a temporal limitation will often be the "preferred method of limiting the scope of a search warrant for a cloud account" because it helps officers to "particularize their searches to avoid general rummaging." *Id.* at 1328. Such limitations address privacy concerns created by the wholesale seizure of digital data, which the Supreme Court warned "would typically expose the government to far *more* than the most exhaustive search of a house." *Riley v. California*, 573 U.S. 373, 396 (2014).

Here, the template Officer Nelson used to draft the iCloud warrant included a list of eleven types of data that virtually authorized the search and seizure of every piece of data that could be found in Rondeau's iCloud account. *See generally* Docket 39 at 22-24. The files to be searched for and seized are not described as those files that constitute evidence of conduct that would give rise to the crime of rape, or indeed, any crime.[2] Rather, the files that the iCloud account could be searched for and seized includes "all subscriber information," "all email content," "all detailed billings records," all photographs and videos, "all location history,"—essentially anything contained within the iCloud account. *See id.* at 23.

The Eighth Circuit's particularity test often focuses on whether the offense under investigation was sufficiently identified and tied to the items to be searched and seized in the warrant. *Sherman*, 372 F. App'x at 676 (holding that a warrant was not overbroad because the search warrant was tied to a specific crime); *United States v. Nieman*, 520 F.3d 834, 839 (8th Cir. 2008) (holding that a warrant that limited items to be searched and seized to those relevant to the charged crime was not overbroad); *Gleich*, 397 F.3d at 611-12 (holding that a warrant authorizing the search of computer files was

[2] While the iCloud warrant stated that the state magistrate judge found probable cause to search the iCloud account because the property is "[p]roperty that constitutes evidence of the commission of a criminal offense;" "[c]ontraband, the fruits of crime, or things criminally possessed; and "[p]roperty designed or intended for use in, or which is or has been used as the means of committing a criminal offense[,]" the warrant does not identify which crime or crimes will be shown by the sought-after evidence. *See* Docket 39 at 22.

sufficiently particular because it limited the officers' search to "items specifically prohibited by statute"); *see also United States v. Good Voice*, 602 F. Supp. 3d. 1150, 1168-69 (D.S.D. 2022) (holding warrant that authorized the search of defendant's entire Facebook account was sufficiently particular because it limited the evidence to be seized to violations of a specific statute and contained temporal limitations). The only limiting provision on the search warrant itself is the reference in the caption to "[i]n the matter of **Rape** in Lincoln County, South Dakota." *See* Docket 39 at 22. Beyond this line in the caption, there is no reference to a victim, statute, temporal condition, or other language in the warrant that would inform officers of what they were allowed to seize. Courts have held that warrants lacking such references are overbroad. *Compare Lindell v. United States*, 82 F.4th 614, 620 (8th Cir. 2023) (upholding the seizure of an individual's entire phone as sufficiently particular where the warrant "described with specificity three federal offenses the government is investigating[,] . . . identified the particular records and information that law enforcement may seize[,]" and where the government "implemented filter protocols to safeguard confidential, private, and privileged matters" on the individual's phone); *with In re Grand Jury Proceedings*, 716 F.2d 493, 497 (8th Cir. 1983) (holding that the scope of a warrant was overbroad, despite including a temporal limitation, where "the warrant did not indicate that the documents sought pertained to any specific transactions, did not identify the offenses on which the evidence was sought, and did not confine the search to any particular files or categories of documents"); *and United States v. Jackson*,

2019 WL 13127190, at *10, 13 (D. Minn. Jan. 4, 2019) (holding that warrant's authorization to seize "[a]ny and all files" stored on a phone was overbroad because the warrant failed to constrain the search and seizure to the specific offense for which the warrant was issued). Further, based upon the searching officers' own understanding that the iCloud warrant authorized a search for "basically anything that was in the iCloud warrant," the reference to a rape in the warrant's caption failed to sufficiently identify and limit the seizure of files to the crime under investigation. *See* Docket 45 at 70-71.

Even if this court were to assume that the caption's reference to a rape is a sufficient limitation, the lack of a temporal limitation, "where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular." *Burkhow*, 2020 WL 589536, at *8-10 (holding that a search of a defendant's entire Facebook account was overbroad because while the warrants only "authorized the government to seize a limited amount of information related to the specific offense[s] under investigation," the court reasoned that "[s]ome reasonable attempt could have been made to narrow the scope of the search, particularly by setting date limitations") (citations omitted). At the evidentiary hearing, it was established that the iCloud account was created in 2011, and Officer Nelson testified that he believed the earliest photograph obtained by officers was dated sometime in late-2020. *See* Docket 45 at 47. It is difficult to conclude that S.R.'s allegations, which indicated that the earliest communication between S.R. and Rondeau took place on June 13, 2022, *id.* at 59-60, justifies the iCloud warrant's request to search and seize all

evidence, from any device, within an 11-year-old iCloud account. Instead, the lack of a sufficient subject matter restriction or circumscribed time window in the iCloud warrant allowed officers to engage in a "general, exploratory rummaging" that the Fourth Amendment seeks to prevent. *Shrum*, 59 F.4th at 973 (quoting *Sigillito*, 759 F.3d at 923); *see also McCall*, 84 F.4th at 1321, 1328 (assuming that an iCloud warrant, which "authorized officers to search seven broad categories of data, essentially encompassing the entirety of [the defendant's] iCloud account" was overbroad where the government conceded the warrant was insufficiently particular because "it allowed a search of all the conceivable data on the account without any meaningful limitation").

Also, even when courts have upheld broad language in describing the items to be seized as sufficiently particular, it is, in part, because officers do not have information as to where specific evidence of a crime is located on a phone or social media account. *See, e.g.*, *Ivey*, 91 F.4th at 917-18 (upholding search of defendant's entire phone for "evidence related to firearms, ammunition, and possession" as sufficiently particular because "[e]vidence of the offense could have been found anywhere in the phone"); *United States v. Bishop*, 910 F.3d 335, 336-38 (7th Cir. 2018) (holding that a warrant's seizure description of "any evidence" related to the crime of dealing illegal drugs was sufficiently particular when officers did not know where the defendant kept such evidence on his phone); *United States v. Alford*, 744 Fed. App'x 650, 653 (11th Cir. 2018) (upholding a warrant to search nearly all data in a Google account because it "was as specific as the circumstances and nature of the

activity under investigation permitted" where the investigators did not know the identity of the perpetrator linked to the account). Under such circumstances, these warrants were not "general warrants" because the "warrant[s] need not be more specific than knowledge allows." *Ivey*, 91 F.4th at 918 (quoting *Bishop*, 910 F.3d at 337-38).

Here, however, such broad language in the iCloud warrant was unnecessary. This is a not a case where "no indication was given regarding the nature of the format in which the sought-for video and photographs were created or stored, [such that] it was necessary to search a broad array of items for the relevant materials." *Summage*, 481 F.3d at 1079-80. Officer Nelson had information that Rondeau had allegedly photographed and taken videos of S.R. using his iPhone. Docket 45 at 32-33. Officer Nelson also had information that the communications between S.R. and Rondeau occurred only on Snapchat and reached back to the date of June 13, 2022. *Id.* at 24. He did not have information that Rondeau made purchases related to the offense with his Apple ID, that any device besides Rondeau's iPhone was used during the offense, or that S.R. and Rondeau communicated through any other app. Unlike the circumstances justifying a search of the defendant's entire phone in *Ivey*, here, "[e]vidence of the offense could [not] have been found anywhere in the phone." *Ivey*, 91 F.4th at 918. Under the present circumstances, because Officer Nelson knew the limited time frame of the offense, and "the precise identity and content of the photos/videos sought," *see United States v. Winn*, 79 F. Supp. 3d 904, 920-21 (S.D. Ill. 2015), the iCloud warrant was insufficiently particular in

its inclusion of all parts of an iCloud account because it was not as "specific [as] knowledge allow[ed]." *Ivey*, 91 F.4th at 918 (quoting *Bishop*, 910 F.3d at 337-38); *see also United States v. Jones*, 2021 WL 960910, at * 4 (D. Minn. Mar. 15, 2021) (reasoning that "general categories of information to search" were sufficiently particular where the Facebook warrant "identified specific categories of information to be searched and seized, and it permitted seizure of data from a relatively narrow time window").

Traditionally, "the generality of a warrant cannot be cured by the specificity of the affidavit which supports it because, due to the fundamental distinction between the two, the affidavit is neither part of the warrant nor available for defining the scope of the warrant." *United States v. Curry*, 911 F.2d 72, 76-77 (8th Cir. 1990) (quoting *United States v. Gill*, 623 F.2d 540, 543 (8th Cir. 1980). "[A] description in a supporting affidavit can supply the requisite particularity if a) the affidavit accompanies the warrant, and b) the warrant uses suitable words of reference which incorporate the affidavit." *Id.* at 77 (quoting *United States v. Strand*, 761 F.2d 449, 453 (8th Cir. 1985)). Here, however, it cannot be said that the warrant incorporated the affidavit by reference. The iCloud warrant mentioned the affidavit only once in its averment of probable cause. *See* Docket 39 at 22. Because "[b]oth the Supreme Court and [the Eighth Circuit] have concluded that a warrant does not incorporate a supporting affidavit when it merely states that the affidavit establishes probable cause," the iCloud warrant did not incorporate the affidavit by reference. *United States v. Szczerba*, 897 F.3d 929, 937 (8th Cir. 2018) (citing

Groh v. Ramirez, 540 U.S. 551, 555 (2004)). Thus, the affidavit cannot be used to overcome the facial overbreadth of the iCloud warrant itself. *See Curry*, 911 F.2d at 77-78.

For the reasons stated above, the court sustains Rondeau's objection and finds that the iCloud warrant was overbroad and not sufficiently particular under the Fourth Amendment.

II. Rondeau's Second Objection: The Magistrate Judge Erred in Concluding the *Leon* Good Faith Exception Applies.

Rondeau also objects to the Magistrate Judge's conclusion that the *Leon* good faith exception to the exclusionary rule applies to the Apple iCloud warrant. Docket 48 at 4.

Ordinarily, the consequence for violating the Fourth Amendment's limitations is suppression of the evidence and its fruits under the exclusionary rule. *United States v. Jackson*, 784 F.3d 1227, 1231 (8th Cir. 2015) (quoting *Fiorito*, 640 F.3d at 345). But the exclusionary rule does not apply "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *United States v. Leon*, 468 U.S. 897, 920 (1984). In assessing an officer's good faith reliance on a warrant, the court must "consider the totality of the circumstances, including what the officer knew but did not include in an affidavit." *Shrum*, 59 F.4th at 974 (quoting *United States v. Farlee*, 757 F.3d 810, 819 (8th Cir. 2014).

"Under the good-faith exception, evidence seized pursuant to a search warrant later determined to be invalid[] will not be suppressed if the executing

officer's reliance upon the warrant was objectively reasonable." *Jackson*, 784 F.3d at 1231 (citing *United States v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007)). Courts must consider "whether a reasonably well trained officer would have known that the search was illegal despite a judge's issuance of the warrant. *Id.* (citation omitted).

> The good-faith exception does not apply in four instances:
>
> (1) when the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge;
>
> (2) when the issuing judge 'wholly abandoned his judicial role' in issuing the warrant;
>
> (3) when the affidavit in support of the warrant is 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;' and
>
> (4) when the warrant is 'so facially deficient' that no police officer could reasonably presume the warrant to be valid.

Id. (quoting *Proell*, 485 F.3d at 341).

Rondeau argues that the third and fourth circumstances apply. *See* Docket 48 at 4-10. Rondeau offers two arguments in support of his claim: (1) a "reasonably well-trained officer" should have known the search was illegal because there was insufficient probable cause to support the breadth of information sought in the iCloud warrant and (2) the warrant was "so facially deficient" in failing to state with particularity the items to be seized that it cannot be reasonably relied upon. *Id.* at 5-7.

The court does not agree that the third circumstance applies here. Rondeau points to the warrant's failure to list a specific crime, the lack of a temporal limitation, and the detectives' knowledge of S.R.'s allegations as indicative of their awareness that the iCloud warrant was overbroad and exceeded its probable cause. *Id.* at 5-6. As noted above, the iCloud warrant authorized law enforcement to search and seize data beyond the probable cause established in Detective Nelson's affidavit. The Eighth Circuit has held that "an officer executing a search warrant may rely [on] the permissibility of the issuing judge's inference that such a nexus exists when that inference has 'common sense appeal.' " *United States v. Perry*, 531 F.3d 662, 665 (8th Cir. 2008) (quoting *United States v. Carpenter*, 341 F.3d 666, 671 (8th Cir. 2003)). Because there were sufficient facts alleged in the warrant affidavit to support the conclusion that there was probable cause to search the iCloud account for support of S.R.'s allegations, this court cannot say that it was unreasonable for Detectives Nelson and Stroschein to rely upon the state magistrate judge's inference of a nexus between the evidence sought and the iCloud account. Although broad, the iCloud warrant was not "so lacking in indicia of probable cause" that it would be unreasonable for officers to conclude the warrant authorized a search for S.R.'s allegations on Rondeau's iCloud account.

The court agrees with Rondeau, however, that the fourth circumstance applies. Despite concluding that the warrant lacked probable cause, the Magistrate Judge felt "constrained to apply *Leon* good faith to Detective Nelson's Apple iCloud search warrant" because of caselaw in *Eggerson*, *Kilman*,

Koech,[3] and *Blake*. Docket 44 at 21-24. Rondeau argues that none of the four cases requires this court to apply the *Leon* good faith exception because each case is distinguishable. Docket 48 at 7-10.

Rondeau argues that the Eighth Circuit's decision in *Eggerson* does not require this court to apply the good faith exception because the iCloud warrant is "so facially deficient that no reasonable officer could presume the warrant was valid." Docket 48 at 7. In *Eggerson*, the warrants authorized officers to seize the defendant's cell phones, "items tending to show possession and/or ownership of firearms such as documentation, and [c]omputers, and all components thereof which would tend to process, compile, store or send information relating to the illegal trafficking or possession of controlled substances." *United States v. Eggerson*, 999 F.3d 1121, 1126 (8th Cir. 2021) (cleaned up). The Eighth Circuit reasoned that the good faith exception applied because "a reasonable officer could have read the warrants to permit him to search and seize cell phones only to the extent they were tied to illegal drug and firearm possession, [thereby] limiting the property to be searched to both the suspect and the crime under investigation." *Id.* Rondeau distinguishes the iCloud warrant from the warrants in *Eggerson* on the basis that the iCloud

[3] As Rondeau correctly points out, the magistrate judge in *Koech* did not discuss application of the *Leon* good faith exception. Docket 48 at 9. The magistrate judge in *Koech* held that the search warrant for the defendant's cell phone was sufficiently particular based on the totality of the circumstances. *United States v. Koech*, 2018 WL 4473530, at *21 (D. Minn. July 17, 2018). As such, this court will not address this case in its discussion of whether the *Leon* good faith exception applies.

warrant fails to "[link] any of the data to a crime" and contains "no mention of any particular crime" beyond the warrant header's reference to a rape in Lincoln County. Docket 48 at 8.

Rondeau provides similar arguments for *Kilman* and *Blake*. In *Kilman*, the district court upheld a search warrant for a defendant's phone where the warrant authorized the search for specific text messages and for "photographs or video of [the victim] or any other children that are either unclothed or partially unclothed." *United States v. Kilman*, 2016 WL 6134546, at *3 (D. Minn. Sept. 6, 2016). In *Blake*, the Eleventh Circuit held that because it was a "close enough question" as to whether a Facebook warrant was sufficiently particular, the warrant was not "so facially deficient" as to preclude officers from reasonably relying upon it. *United States v. Blake*, 868 F.3d 960, 975 (11th Cir. 2017). Rondeau distinguishes the iCloud warrant from the warrant in *Kilman* on the grounds that the warrant was limited to "specified evidence of a crime rather than a generalized list of all available data." Docket 48 at 8. Similarly, Rondeau argues that while the Facebook warrants in *Blake* required disclosure of "virtually every type of data that could be located in a Facebook account," the warrants limited the information seized to "data that 'constitute[d] fruits, evidence and instrumentalities' of a specified crime." *Id.*; *Blake*, 868 F.3d at 966-67. Rondeau concludes that because the iCloud warrant here fails to particularly limit the seizure of items to a specific crime, the warrant is "so facially deficient" that no reasonable officer can rely upon it. *See* Docket 48 at 7.

The iCloud warrant here can be distinguished from the cases discussed above. The overly broad nature of the iCloud warrant, while similar in scope to the authorized warrants in *Eggerson*, *Kilman*, and *Blake*, was not tempered by a limitation that would guide officers on what data law enforcement could seize after Apple's broad disclosure. The *Eggerson* warrant limited the files to be seized to evidence of illegal drug and firearm possession, *see Eggerson*, 999 F.3d at 1126, the *Blake* warrant explicitly provided that law enforcement could only seize data that "constitute[d] fruits, evidence and instrumentalities of a specific crime," *Blake*, 868 F.3d at 967, and the *Kilman* warrant was specifically limited to seizing digital evidence that constituted child pornography, *see Kilman*, 2016 WL 6134546, at *4. In comparison, the iCloud warrant here was broader than the warrants in *Eggerson*, *Kilman*, and *Blake* because it failed to provide any limitation of what law enforcement could seize from the iCloud account.

If Detectives Nelson and Stroschein had limited their search to S.R.'s allegations and relied upon the reference to a rape in the warrant's caption in conducting their search, the good faith exception could apply because Detective Nelson was the same officer who drafted and executed the iCloud warrant, probable cause existed to search for evidence of S.R.'s allegations on the iCloud account, and in the context of the rest of the warrant, Detectives Nelson and Stroschein could form a reasonable belief that the warrant was limited to the seizure of items related to S.R.'s allegations. *See United States v. Henderson*, 416 F.3d 686, 695 (8th Cir. 2005) (applying good faith exception because

probable cause existed for the search, "the officer who requested the warrant was the same officer who executed it," and "in the context of the rest of the warrant, the officer had a reasonable belief that [the] warrant was limited to the seizure" of evidence of the crime under investigation); *United States v. Harris*, 2021 WL 3929270, at *4 (D. Minn. Sept. 2, 2021) (holding good faith exception applied where the same officer drafted and executed the warrant and was "fully aware of the purpose and parameters of the investigation," despite the fact the warrant failed to refer to a search for gun-specific evidence). Additionally, both Detectives Nelson and Stroschein testified that they were specifically looking for images of S.R. *See* Docket 45 at 19-20, 70; *see also United States v. Armstrong*, 2024 WL 2894273, at *25 (D. Minn. Mar. 12, 2024) (holding that good faith exception applied to an overbroad warrant where the officer "had the belief that the warrant was issued for him to specifically search for evidence relating to the selling of drugs and the illegal possession of firearms"). An issue exists, however, because Detectives Nelson and Stroschein did not limit their search to the crime under investigation. *Strand*, 761 F.2d at 456 (explaining that the *Leon* good faith exception only applies in cases where officers have "acted within [the] scope" of a search warrant).

For instance, despite knowing the date of the alleged crime, and that the earliest reported communication between the victim and Rondeau was within two days of the alleged crime, Detectives Nelson and Stroschein searched through the entirety of the iCloud data without regard to a temporal limitation. *See* Docket 45 at 19. And despite "mostly searching photos and videos," the

officers' chosen method of analyzing the data—divvying up the files and clicking each one to see what it contained—makes little sense when the probable cause established in the warrant's affidavit implicitly limited the items to be seized to a relatively short time frame. *See id.* at 19, 43, 46. Further, while Detective Stroschein testified that she reviewed the iCloud warrant and affidavit around the time she began her search, Detective Stroschein stated that she could search and seize "[b]asically anything that was in the iCloud account." *Id.* at 70. Detective Stroschein also indicated that she knew the warrant did "not specifically" allow officers to look for evidence related to T.C.'s allegations, but it was her understanding that she could open any piece of data within the iCloud account. *Id.* at 76. It is not objectively reasonable for officers to conclude that the iCloud warrant, which authorized the search and seizure of an iCloud account created eleven years prior, should give them unbridled discretion to search for and seize whatever they wish without being limited to the crime under investigation. *United States v. Armstrong*, 2022 WL 17417901, at *19 (D. Minn. Sept. 2, 2022) (reasoning that because a cell phone search exposes the government to a broad array of information that is tempered by the particularity requirement's prohibition against general rummaging, "no law enforcement should reasonably believe that they could search for, seize, and keep the unrestricted sets of files sought by the [s]earch [w]arrants (which were not limited to evidence of a particular crime)").

Here, the investigation arose from S.R.'s allegations. The affidavit supporting the iCloud warrant is directed toward searching for and seizing

photos and videos of S.R., and communications between S.R. and Rondeau. *See* Docket 39 at 15-16. Detectives Nelson and Stroschein testified that they had no reason to believe that communications between S.R. and Rondeau went any further back than June 13, 2022. Docket 45 at 24, 74. Before beginning their search of the iCloud data, both Detective Nelson and Detective Stroschein testified that they knew of T.C.'s allegations. *See id.* at 42, 67-69. During her search of the iCloud account, Detective Stroschein indicated that the pinpoint of the Plucker Waterfowl Production area triggered a connection to T.C.'s allegations. *Id.* at 76. Detective Stroschein also testified that there were three unopened linked files "right along next to the screenshot." *Id.* Instead of obtaining an additional search warrant, Detective Stroschein clicked on the three links, which contained videos of a female urinating in a wooded area that were later confirmed to be T.C. *Id.* at 69-70.

In similar cases where officers have discovered evidence of an unrelated crime on a digital device, the Eighth Circuit has upheld searches of the unrelated evidence where officers have obtained an additional warrant. *See United States v. Hudspeth*, 459 F.3d 922, 927-28 (8th Cir. 2006), *rev'd in part on other grounds*, 518 F.3d 954, (8th Cir. 2008) (en banc) (holding that officers did not exceed the scope of original warrant authorizing the seizure of evidence of illegal drug activity on defendant's computer where after discovering child pornography, officers stopped the search and obtained a second warrant authorizing the search for child pornography); *United States v. Koch*, 625 F.3d 470, 476 (8th Cir. 2010) (upholding seizure of child pornography on

defendant's flash drive where officers unexpectedly encountered child pornography and only continued searching for child pornography after obtaining a new warrant); *United States v. Suing*, 712 F.3d 1209, 1212 (8th Cir. 2013) (holding officer did not continue "a new, extended search for child pornography without judicial authority" while searching for evidence of illegal drugs on the defendant's computer hard drive where officers "stopped the search, called a prosecutor for advice, and obtained a new warrant authorizing the search for child pornography").

Because the officers understood that they could search for anything within the iCloud account and they relied upon the unparticularized list of items in the iCloud warrant to justify the search for T.C.'s allegations, the officers' actions were unreasonable when they failed to seize evidence related only to the crime under investigation. The warrant and warrant affidavit failed to provide an officer with the reasonable belief that the iCloud warrant authorized a search for T.C.'s allegations because neither makes any reference to T.C.'s allegations. *See* Docket 39 at 13-24. Because the iCloud warrant was not tailored to the facts of the case, the description of items to be seized was left glaringly broad and allowed officers to conduct a general rummaging of Rondeau's iCloud account. Thus, it is not objectively reasonable for an officer to conclude that they may seize digital data without regard to the crime under investigation. *See Armstrong*, 2022 WL 17417901, at *19.

Despite *Leon*'s language that the good faith exception only applies when officers act within the scope of a warrant, *see Leon*, 468 U.S. at 922, the Eighth

Circuit has applied the good faith exception when searching officers made an "honest mistake" in exceeding the scope of the warrant. *See Shrum*, 59 F.4th at 974 (quoting *United States v. Suellentrop*, 953 F.3d 1047, 1050 (8th Cir. 2020)). Thus, under *Shrum*, the good faith exception allows the "admission of evidence obtained by officers who 'reasonably believed that the warrant authorized the search, even if their interpretation was mistaken.' " *Id.* (quoting *Suellentrop*, 953 F.3d at 1050). Because it is hard to curb honest mistakes made by officers through exclusion, the exclusionary rule applies to behavior that is "deliberate," "reckless," or "grossly negligent" with respect to the Fourth Amendment. *Herring v. United States*, 555 U.S. 135, 144 (2009).

Here, however, it is difficult to conclude that the searching officers made an "honest mistake" when they specifically searched for and seized evidence related to T.C.'s allegations. Detective Stroschein clearly intended to search for evidence of a crime unrelated to S.R.'s allegations by requesting the police report detailing T.C.'s allegations from the Tea Police Department. Docket 45 at 67-68. While it is unclear from her testimony whether she reviewed the report first or if she discovered the screenshot of the Plucker Waterfowl Production area and three videos first, *id.* at 68-69, the record indicates that the searching detectives did not unexpectedly stumble upon evidence of an unrelated crime because both detectives began to search the iCloud account with knowledge of T.C.'s allegations against Rondeau. Instead of solely searching for photos and videos of a rape for the only named victim in the iCloud warrant's affidavit, Detective Stroschein abandoned the search for evidence of a rape as related to

S.R. and began a search and seizure of evidence she believed was connected to a completely unrelated crime. *See Winn*, 79 F. Supp. 3d. at 925-26 (finding that officers did not act in good faith reliance on a warrant authorizing a search of a defendant's phone where they discovered unrelated child pornography and "essentially abandoned their search for evidence of public indecency in order to follow the trail of evidence for the new crimes" without first obtaining another warrant).

After a review of the facts in this case, this court cannot say that the detectives' reliance on the iCloud warrant to search for evidence of T.C.'s allegations was objectively reasonable. An objectively reasonable officer would conclude that they do not need to look at every piece of data in an 11-year-old iCloud account to find photos and videos of S.R. taken on June 15, 2022. Further, based on the officers' own understanding of the broad scope of the iCloud warrant, the court concludes that the iCloud warrant was "so facially deficient" such that no executing officer could reasonably rely upon it because it authorized an exploratory, general rummaging of Rondeau's iCloud account.

For the above reasons, the court sustains Rondeau's objection and concludes that the *Leon* good faith exception does not apply to the iCloud warrant in these circumstances.

III. *Miranda*

In the Report and Recommendation, the Magistrate Judge recommended that Rondeau's statements in response to questions "about the location of his phone, truck, or other aspects of the alleged crime while in custody and prior

to the advisement of his *Miranda* rights" should be suppressed. Docket 44 at 15. Rondeau and the Government do not object. *See* Docket 48. After a de novo review, this court adopts in full the Magistrate Judge's recommendation that Rondeau's statements made to officers before he received *Miranda* warnings should be suppressed.

CONCLUSION

ORDERED that the Report and Recommendation (Docket 44) is adopted in part and rejected in part, and Rondeau's motion to suppress (Docket 30) is granted.

Dated November 13, 2024.

BY THE COURT:

/s/ *Karen E. Schreier*
KAREN E. SCHREIER
UNITED STATES DISTRICT JUDGE